
# Multinational Experiment 7
# Outcome 3 – Cyber Domain
# Objective 3.4

# Cyber Situational Awareness Standard Operating Procedure

Version 1.0

01 December 2012

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **08 JUL 2013** | **N/A** | |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Multinational Experiment 7 Outcome 3 - Cyber Domain Objective 3.4 Cyber Situational Awareness Standard Operating Procedure** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **JOINT STAFF-MN//ACT Integration 116 Lakeview Parkway Suffolk, VA 23435** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release, distribution unlimited.**

13. SUPPLEMENTARY NOTES
**The original document contains color images.**

14. ABSTRACT
**The Cyber SA SOP provides structures, roles, processes and tool requirements for gaining and maintaining effective SA. The Cyber SA SOP supports decision makers in gaining an understanding of activities in cyberspace. The Cyber SA SOP is supported by utilizing technologies that enable collection, analysis, presentation, and sharing of information related to cyberspace. A balance of automated processes along with human decision making is enabled by fusing and analyzing recognized data patterns, along with collaborative functions to share this information.**

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **UU** | **23** | |

# CYBER SITUATIONAL AWARENESS STANDARD OPERATING PROCEDURE

Reference:

A. MNE7 Campaign Lexicon, draft version 0.4, dated 28 November 2011.
B. MNE7 Objective 3.3 Guidelines for Decision makers, dated 16 APR 2012.
C. MNE 7 Objective 3.5 Concept of Employment for Cyber Situational Awareness Within the Global Commons, draft version 0.5, Dated 02 Apr 2012.
D. MNE 7 Objective 3.2 Information Sharing Framework, version 1.0, dated 20 April 2012.

## PART 1 - INTRODUCTION

### BACKGROUND

1. The Cyber Situational Awareness Standard Operating Procedure (Cyber SA SOP) developed during the Multinational Experimentation 7 (MNE7) campaign (2011 – 2012) is the primary product of the cyber enabling technologies Objective 3.4. The objective is led by Finland, and is a part of the MNE7 Outcome 3 Cyber domain activity focused on cyber situational awareness (SA). Objective 3.4 is supported by contributing nations Austria, Denmark, Germany, Italy, Norway, Poland, Sweden, Switzerland, United Kingdom, the United States of America and NATO ACT.

2. The Cyber SA SOP provides structures, roles, processes and tool requirements for gaining and maintaining effective SA. The Cyber SA SOP supports decision makers in gaining an understanding of activities in cyberspace. The Cyber SA SOP is supported by utilizing technologies that enable collection, analysis, presentation, and sharing of information related to cyberspace. A balance of automated processes along with human decision making is enabled by fusing and analyzing recognized data patterns, along with collaborative functions to share this information.

### AIM

3. The Aim of the SOP is to describe how to establish, maintain and share situational awareness (SA) in a generic, governmental level cyber centre. It describes what information, reporting and collaboration is needed to build cyber awareness and to inform other relevant stakeholders - especially senior leaders and decision makers. The SOP also represents technology requirements and implementation challenges.

### DEFINITIONS

4. There is no coherent and agreed lexicon or taxonomy that supports cyber domain situational awareness across governments, agencies, allies, industry and academia. MNE7 has therefore produced a Campaign Lexicon (Reference A) to enable coherent progress of MNE7 outcomes and objectives through common understanding. The definitions used in this SOP are listed in Annex A.

## SCOPE

5. The Cyber SA SOP only focuses on the parts related to cyber situational awareness within the cyber center functionalities. The execution part of the cyber center is out of scope of this document, but understood as an important co-functionality. The Cyber SA SOP does not address any legal aspects although information related to legal aspects may be of value in the SA establishment processes.

## ASSUMPTIONS

6. The SOP assumes an unconstrained internal information sharing environment.

7. The SOP addresses defensive cyber operations only.

8. A dynamic systems view or map must exist.

# PART 2 - FRAMEWORK

9. Figure 1 illustrates the framework for the Cyber SA SOP. The cyber center in this document is a generic governmental level cyber center, however, the functionality of the cyber center can be deployed within other more specific contexts as well. The cyber center collects information from various sources, analyzes the information to gain situational awareness, and communicates the information to relevant parties. In cases needed, the cyber center may coordinate activities between the ICT operators and partners as well as bring major incidents to the attention of higher level decision makers. The generic cyber center consists of two main functions: situational awareness and activity coordination (for example, SOC management).

10. In Reference D the information sharing framework represents a hub & node model in which information flows between a central capability, the hub, and the end-point of a branch in a network or a point at which two or more branches meet, the so called nodes. In Figure 1, the cyber center is such a hub collecting and sharing information from several sources, for example, the SOCs of ICT operators, other cyber centers, and sources from different domains.

11. The cyber center collects information from ICT Operators, partners, and other cyber centers. An ICT Operator is an organization that operates information systems or networks, for example, critical infrastructure operators (energy, communication, finance, health, etc.), private companies and governmental entities. A partner may be an organization that provides other relevant information that is useful for assessing the overall threat level or bring added value to the situational awareness, for example, intelligence agencies, law enforcement or private sector consultancy. The cyber center would also exchange information with other cyber centers, for example, as part of international collaboration. In some cases, also individuals may provide information relevant to the cyber center.

12. The cyber center fuses and analyses the collected information in order to achieve improved situational awareness. The situational awareness is communicated to the relevant ICT operators and partners. In case needed, the cyber center may coordinate actions between the parties as part of cyber incident handling. The cyber center may direct the action of all national effectors and coordinate media communication in case of a cyber crisis.

13. The cyber center informs decision makers about abnormal cyber activities and makes recommendations where appropriate on possible course of actions and cyber responses. The cyber center follows policies and orders, and receives guidance and upper level situational information from the decision makers.

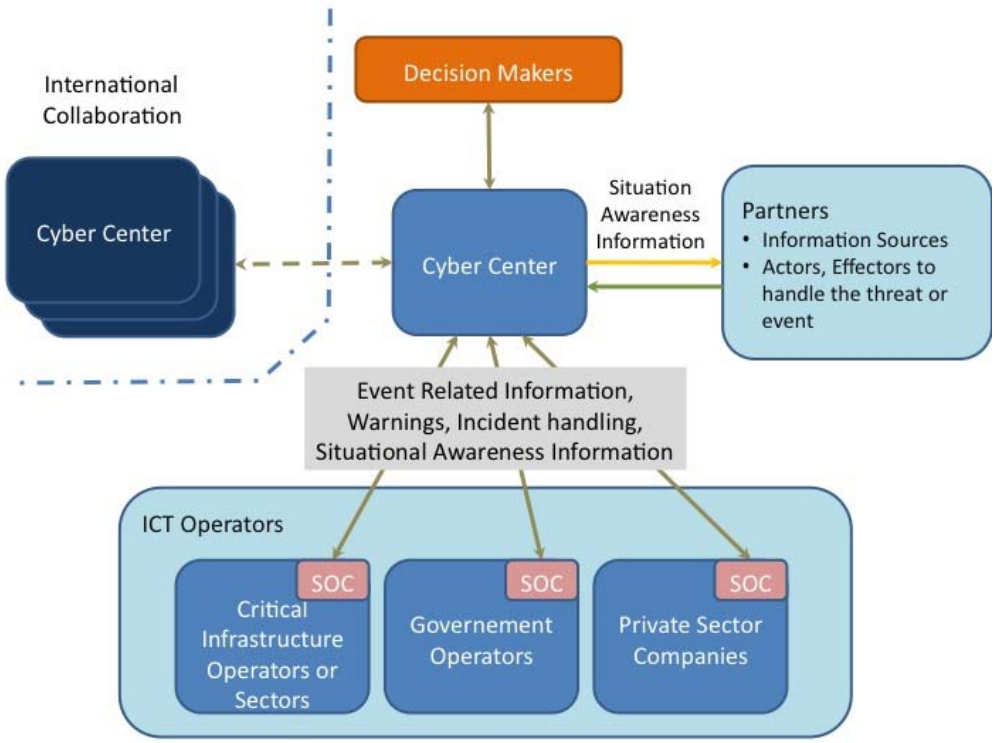


**Figure 1. The framework of the Cyber SOP.**

14. The purpose of the cyber center is not to take CERT (Computer Emergency Response Team) responsibilities or replace existing CERT organizations and structure. Today there is a global network of CERT organizations (governmental, organizational, and institutional). CERT tasks include preventing, observing, and solving information security incidents and disseminating information on threats to information security. The cyber center has a wider operational responsibility to understand cyber activities to protect critical infrastructure and services. Thus, the cyber center is responsible of providing cyber situational awareness from all aspects; risk management, vulnerabilities, critical assets, threats, impacts on operations etc.

# PART 3 - CYBER SITUATIONAL AWARENESS ROLES

15. This part describes the roles of the main actors presented in the framework. The role descriptions are notional.

## CYBER CENTER

16. The cyber center SA element (function) receives, analyzes and visualizes information, and reports essential issues to the senior level decision makers. The cyber center SA element establishes an understanding of cyberspace activities for its organizations and shares analyzed information with all relevant stakeholders.

17. Tasks of the cyber center SA element include:
- Provide incident reporting policy for the ICT operators
- Information gathering from ICT operators and other sources
- Information analysis
- Building situational awareness of threats and activities in the cyber domain
- Information sharing and collaboration with others
- Reporting (including estimates and recommendations) to decision makers
- Maintain SA data storage and knowledge base for ICT operators

18. The cyber center execution element (function) coordinates required actions to protect and restore services around the network.

19. Tasks of the cyber center execution element may include:
- Distribute recommendations
- Direct actions of all national effectors
- Talks to the media during cyber crisis

20. The cyber center communicates with the partners through resilient communication means and disposes of resilient information systems.

## ICT OPERATORS

21. An ICT Operator is an organization that operates information systems or networks, for example, critical infrastructure operators (energy, communication, finance, health, etc.), private companies and governmental entities. The ICT operators typically have a system operation center (SOC) including responsibilites related to information security and incident handling.

22. The SOC has the capability to monitor, analyze and configure its own networks and/or services using passive and active measures to prevent and limit the effect of cyber incidents.

23. Tasks of the SOC include:
- System maintenance and management including applying the directed security policy and procedures
- Service and network system monitoring

- Provides information including reporting to cyber centers
- Implement directed countermeasures for incident handling/ damage containment
- Incident prevention, incident identification and handling/analysis including:
    - Patch Management
    - Event monitoring
    - Event prioritization
    - Collaboration with other SOCs in accordance with given information exchange policy

**PARTNERS**

24. Partners may include organizations that may provide information that is of added value when forming situational awareness. Such organizations may be, for example, intelligence agencies, law enforcement, private sector consultancy, and in some cases individuals.

**DECISION MAKER**

25. Senior level decision makers are responsible for making decisions regarding the course of action that is considered appropriate in the situation at hand. In order to make decisions, the decision makers need situational awareness to be presented so that it is meaningful in a larger context as well as recommendations on possible responses.

26. Tasks of the decision maker level include:
- Timely decision making related to all operating environments
- Operation oversight
- Prioritizing of activities
- Creating response threshold policies in different scenarios

27. The Decision Maker's Critical Information Requirements (DMCIR) should be established (and regularly reviewed) in order to guide collection efforts as well as to determine level of effort of analysis. DMCIR is a basis for information collection, analysis and reporting in a cyber center. DMCIR sets a focus to all actions taken, and it helps the cyber center to provide relevant situational awareness for decision makers.

# PART 4 - CYBER SA PROCESS MODEL

28. The cyber SA process model is a generic process model for a cyber center. The purpose for a generic approach is to avoid too limited use cases into which this SOP could be applied.

29. A process model illustrated in Figure 2 is used as a reference model to the cyber SA. The model consists of input, processing, storage and output elements. The input element simply feeds the processing element, which then produces output. For the processing, some information and history storage is needed. The feedback arrow shows connections between output and input, which means that the output has effect to input information. Also, inside the cyber center some feedback loops exist. This means that the output from a subprocess may affect inputs of the previous subprocesses.

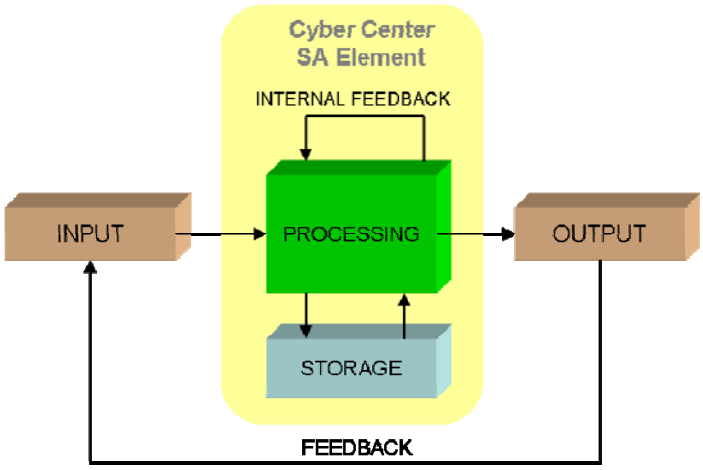


**Figure 2. The generic process model.**

30. The cyber SA process model is presented in Figure 3. The processing phase includes three subprocesses that are collection, detection/assessment, and informing. In Reference C, the collection phase is already included in the detection, but in the cyber center SA process model the collection phase is separated. For the entire SA process, the knowledge of the environment is critical.

31. The input element includes all the information sources available for establishing cyber SA. Input sources are mainly ICT operators and partners, other cyber centers and higher level decision makers.

32. The output element includes all products and information which is provided for stakeholders. The output element of the model does not include those products that are only used internally inside the cyber center.

33. The processing part of the model includes all the activities taking place between input and output. The processing is described in more detail in the following sections, but it mainly consists of information collection, detection, analysis, visualization, and sharing. The process uses storage functions (e.g. databases, and libraries) to generate knowledge and understanding in all phases.

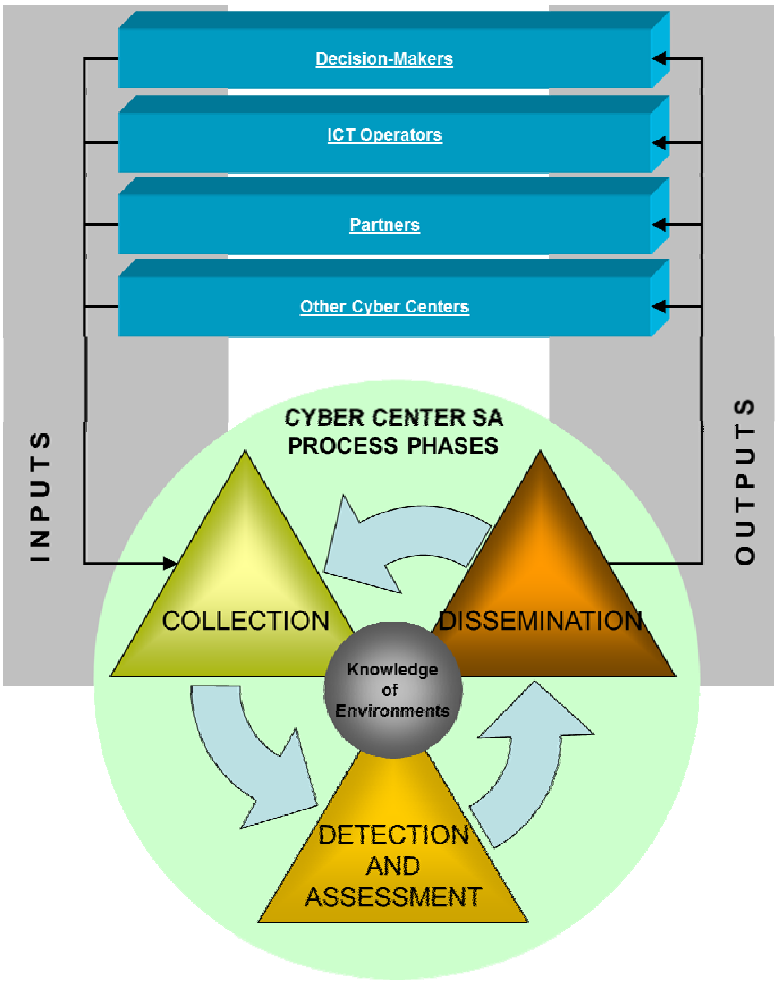


**Figure 3. Cyber center SA process model.**

## INPUTS

34. To generate complete cyber SA, all available and relevant information sources should be utilized. The cyber center receives information about cyber events, incidents and other activities which are relevant to cyber SA from the ICT operators and other partners. The cyber center should continuously evaluate the quality and timeliness of information as well as the reliability of the information sources.

35. The decision makers gives tasks and other guidance to the cyber center. The tasks may include, for example, defensive goals in relation to service and network availability.

36. To support cyber SA, the cyber center should take into consideration information collected from the other domains. The cyber center requires information from other domains to evaluate and synchronize actions in cyberspace to the actions taking place in the other domains.

37. Other cyber centers are also necessary SA information sources. Activities in cyberspace change fast and cyber events may have wide impacts. Thus, information from the other centers helps the cyber center to study the consequences of an event in a larger perspective. Other

cyber centers share vulnerability reports and other relevant information to protect infrastructure and services.

**OUTPUTS**

38. One important stakeholder for the cyber center is the decision maker. Therefore it is crucial to understand the cyber information needs of a decision maker, and thus the previously described DMCIR must be generated. In Figure 4, an analytical model of possible cyber activity elements (columns) is illustrated. The model is created to understand all important elements for senior leaders when making decisions on cyber issues. The model was originally developed to support decision making from a legal perspective, but the elements also apply to other aspects in decision making. The other relevant aspects may include operational context, such as political, economical, military operations, or media aspects.

| Context | Actor | Source Cyber Node | Transit/ Location | | Assessment of Activities | Targets/ Objectives | Consequences | Extent |
|---|---|---|---|---|---|---|---|---|
| Peacetime | State | State | Near Network | Physical Layer | Cyber Attack | State | Casualties | Small |
| Crisis | Terrorist | Military | Mid Network | Logical Layer | Cyber Defence | Military | Physical Damage | Mild |
| Armed Conflict | Person/Entity | Private | Far Network | Social Layer | Cyber Exploitation | Private | Non material | Large |
| | Undetermined | Undetermined | | | Undetermined | Critical Infrastructure | Economic Damage | |
| | | | | | | Civilian Infrastructure | OPSEC | |

**Figure 4. An analytical model of possible cyber activity elements (see Reference B).**

39. The outcomes of the cyber center developed for decision makers should consider all the elements described in the table. Depending on the operational context the importance of each element may vary.

40. The outcomes of the cyber center include information about the current and projected state of the critical infrastructure, critical services, actual cyber activities, and related risks. The information encompasses statistics, geographical locations, traffic volumes, identification status, interconnections, etc. in order to give situational awareness. Situational maps should be scalable so that different resolutions can be considered. The information provided should illustrate and synchronize all six layers of cyberspace (see Reference C). The layers are social, people, personal, information, network, and real world. The cyber center also produces and stores a knowledge base of past activities.

41. Parts of the outcomes of the cyber center are also shared with the ICT operators, partners, and the other cyber centers depending on the relevance and sensitivity of the information to the various stakeholders.

## PROCESSING

42. Processing includes all necessary actions to generate outputs from inputs. Although the SA process described in this document is very straight forward, in real-life the process may be very complex and ad hoc type. The purpose is to give a rough process model outline from which each actor may modify their own detailed SA process phases for a certain cyber center.

### Collection

43. The collection phase consists of all the means required to gather relevant data. Table 1 presents activities, tasks, input, and output for the collection phase. The subphases are information gathering, categorization, and aggregation.

44. During the information collection phase, the cyber center gathers, categorizes, and aggregates information from all relevant sources

45. Categorizing is meta tagging information in order to handle it in a proper way. The categorization and formats may change according to the cyber policies, warning sources, and other guidance. Thereby existing data categorization and format databases should be updated frequently. Information is meta-tagged and/or indexed according to updated categories.

46. In the aggregation phase, information is indexed and appended to knowledge databases. Finally, information is sorted by category.

47. The output from the collection phase is a coherent and structured knowledge database for the next process phase.

**Table 1. The collection phase.**

| Process phase | Activities | Tasks | Inputs | Output |
|---|---|---|---|---|
| 1.1 Collection | 1.1.1 Receive information from all sources | 1.1.1.1 Receive information from SO | Anomalies (TBD) | Coherent and structured database for cyber activity<br><br>Network and service status information<br><br>Network diagrams |
| | | 1.1.1.2 Receive information from D-Ms | Policy<br>Guidance<br>Thresholds<br>(TBD) | |
| | | 1.1.1.3 Receive SA information from Other Domains | Business and system degradations (Anomalies) | |
| | | 1.1.1.4 Receive information from Other Cyber Centers | "Cyber Information"<br>- Threat sources<br>- Attack vectors | |
| | 1.1.2 Categorize | 1.1.2.1 Update data categorization and format | Existing categories and formats<br>Policy, guidance<br>CERT warnings | |
| | | 1.1.2.2 Metatag/index data according to updated categories | Data from 1.1.1<br>Categories from 1.1.2.1 | |
| | 1.1.3 Aggregate | 1.1.3.1 Append data to information database | 1.1.2.2 | |
| | | 1.1.3.2 Index and sort by category | 1.1.3.1 | |

Detection and assessment

48. During the detection and assessment phase, cyber activity information is analyzed. The purpose is to create an understanding of cyber activities and to generate plans and recommendations to the stakeholders. The cyber center recognizes anomalous activity based on the collected and aggregated reports from the previous phase. The analysis consists of four main tasks: creating reference activity baselines, comparing cyber activity information against the reference baselines, indentifying variances and threats, and conducting risk assessment (see Table 2).

49. The parameters and the means of monitoring them should be defined in the reference database. The policies received from the higher level may set some thresholds and high level norms, but creating the reference baseline is the responsibility of the cyber center. The control objectives are set for both long and short term.

50. Gaining and maintaining cyber SA requires management of large volumes of structured and unstructured data, the ability to continuously check against reference activities, analyze the data, and recognize and identify anomalies.

51. Risk assessment is divided into four categories as seen in Table 2.

52. The output of the phase is a set of plans, maps and recommendations. The phase products a risk map, contingency and prevention plans, Continuity of Operations Plan (COOP), and resilience requirements.

**Table 2. The detection and assessment phase.**

| Process phase | Activities | Tasks | Inputs | Output |
|---|---|---|---|---|
| 1.2 Analysis | 1.2.1 Create/update normal cyber activity baselines | 1.2.1.1 Identify data elements/attributes/thresholds/measurement periodicities | | Risk Map<br>Contingency Plan<br>COOP<br>Prevention Plan<br>Resilience Requirements<br>Trends (short/long term)<br>Visualized SA pictures<br>Simulations |
| | | 1.2.1.2 Calculate control limits<br>- long term<br>- short term | | |
| | 1.2.2 Compare data against baselines | 1.2.2.1 Identify high outliers | | |
| | | 1.2.2.2 Identify low outliers | | |
| | 1.2.3 Identify variances between current activity and baseline | 1.2.3.1 Identify long term trends (+/-) | | |
| | | 1.2.3.2 Identify short term anomalies (+/-) | | |
| | 1.2.4 Conduct Risk Assessment | 1.2.4.1 Life, health and environment | | |
| | | 1.2.4.2 Economics/Monetary | | |
| | | 1.2.4.3 Mission Effectiveness | | |
| | | 1.2.4.4 Related or inter-related organizations | | |

Dissemination

53. The dissemination phase includes all the activities and tasks related to providing information to appropriate stakeholders. The phase consists of two main activities: categorizing information and sharing information (see Table 3).

54. The purpose of categorizing information is to classify the resulting outcome of the analysis phase so that the proper products are sent to the proper stakeholders. To do that stakeholder data categorizing and formats are updated. The outcome is addressed, tagged and formatted according to the updated categories.

55. The final activity of the cyber center SA process model is to provide produced information and outcomes to relevant stakeholders using adequate communication means.

**Table 3. The dissemination phase.**

| Process phase | Activities | Tasks | Inputs | Output |
|---|---|---|---|---|
| 1.3 Informing | 1.3.1 Categorize information | 1.3.1.1 Update end-user data categorization and format | Risk Map<br>Contingency Plan<br>Continuity of Operations Plan (COOP)<br>Prevention Plan<br>Resilience Requirements | |
| | | 1.3.1.2 Metatag/format/address data according to updated end-user categories | | |
| | 1.3.2 Send information end-user | 1.3.2.1 Send information to system operators | | |
| | | 1.3.2.2 Send information to decision-makers | | |
| | | 1.3.2.3 Send information to other domains | | |
| | | 1.3.2.4 Send information to other cyber centers | | |

## INFORMATION QAULITY AND FORMAT REQUIREMENTS FOR CYBER SA PROCESS

Information quality attributes

56. Several information quality and format requirements could be set for establishing understandable SA in the cyber center. Information quality is a measure of the value which the information provides to the user of that information. Quality is often recognized as subjective and the quality of information can then vary among cyber stakeholders and among uses of the information. However, a high degree of quality increases its objectivity or at least the intersubjectivity. Information quality attributes can be defined from different aspects (e.g. contextual, representational, intrinsic). In this document the contextual approach is used, and thus information quality attributes are relevancy, accuracy, timeliness, completeness and amount of data.

57. Relevancy means that information has significance. The cyber center should gather only information that contributes to cyber SA establishment. Thus, the cyber center defines requirements for reporting.

58. Accuracy of the information is related to the reliability and capability of the source, which can be either human or technical.

59. Timeliness is an important requirement for cyber information. In cyberspace, events occur rapidly. Therefore, delays in gathering and sharing information should be minimized.

60. Completeness means that as much information as possible related to a given case is gathered and collected. The aim is that all relevant information of a case is available in order to gain better understanding of the situation.
61. Amount of data means that the cyber center has enough data to create complete SA. One of the challenges may be how to filter relevant data from huge databases, and how to create information and knowledge from that data.

Information formats

62. Standardized information formats are necessary when automated information processing is developed. A standardized format makes an information system to be able to process data by using specified data structures and field contents. Structured data also helps manual processing as an operator know which information is included in each part or field of an information message.

63. In this section, some general requirements are presented and discussed. The purpose is not to give exact technical requirements to use certain format but more advise which aspects must be taken account when building information sharing capabilities. Current data interchange formats, especially those developed specifically for the cyber domain, should be taken into account when developing the required standards.

64. A significant part of cyber reporting includes natural language text. Since some incidents may involve actors from different countries and geographic regions, reporting should use agreed character sets and encodings. Information messages should represent time in such a way that it is possible to easily correlate information reported from different time zones, for example, UTC (always maintaining time zone information).

65. Incident information must evolve with time as further analysis is carried out. Different parts of an incident information report may include information of varying degrees of sensitivity. Subsets must be labeled with their appropriate sensitivity.

66. Information sharing systems must be flexible enough to support various degrees of completeness and accuracy while still clearly defining the minimal information required for describing an incident. In general, the SOC incident reports should include:

- Name of the source and target
- The description of various aspects of the source and target
- The description of the methodology used by the attacker
- The identification of the creator of the incident report
- The source of each component of the incident report if it is different from the creator (e.g., the team handling the incident)
- A description of the impact of the incident.
- A description of the actions taken during the course of handling the incident.
- Releasability of the incident report

## SECURITY CONSIDERATIONS

67. All relevant information security measures should be taken to ensure secure processing, distributing, and storing of information. Information security must be considered from legal, process and technical aspects.

68. National and international information security legislation and policies set limitations to information sharing. Security agreements need to be made between the various stakeholders to ensure that the information is handled properly.

# PART 5 – TECHNOLOGY REQUIREMENTS AND GAPS

69. The cyber SA process is supported with appropriate technologies and tools. Figure 5 illustrates a categorization of tools supporting the SA process phases. The arrows in the figure show data flow directions. Typically, analysis and data synthesis tools pull data from storages and after processing push the data back to the storage. Some of the tools only process data but do not save the processed data into the database.

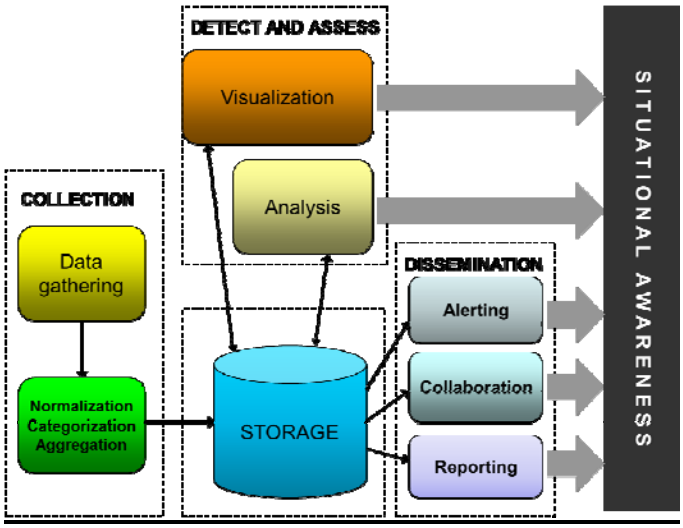


**Figure 5. The categorization of cyber center tools.**

70. In the following paragraphs, requirements for the tools are defined. The requirements are at a general level and describe functionalities that should be available with each tool or set of tools. The implementation challenges are also considered later on.

71. Current technologies already support at least some of the required functionalities, but there are still lots of requirements that need to be addressed. Even if there are technologies available, common data formats and configurations must be agreed to provide interoperability.

## INFORMATION GATHERING

72. Technology requirements for collecting data and information are described by the following activities: gathering and receiving data and information; normalization; categorization; aggregation; and storage. Gathering and receiving data may be performed by both 'push and pull' methods from public or private trusted or untrusted sources. Sources may be traditional (cyber incidents and events, network flows information, news-streams, intelligence reports etc) or untraditional, such as existing and emerging social media applications (such as micro-blogging websites) which are usually less controlled and may be from untrusted sources.

73. The requirements include the ability to monitor data from relevant systems to alert or warn of any changes to the status or availability. This will also include gaining information on regular or large-scale system intrusions; the health and failure of critical systems; identification, transfer

and temporary secure storage of anomalies; and knowledge of the status of system configuration and management.

74. Data and information collected can vary in both format and type. The format can be standardized, freeform, and include either structured or unstructured data. The type may vary with inclusion of text, computer code or language, image/video or any combination of these. Normalization is the process of transforming that data in common format for further processing (without losing the original information), establish baselines and spot anomalies in the incoming data.

Gathering & Receiving Information

75. The technologies must be able to gather and receive data through trusted, interoperable routes and platforms using an open architecture to be able to cope with changes and evolution in cyberspace. Transmission must ensure authentication and confidentiality of sensitive data. The technologies must support data collection from a large number and variety of sources in parallel at near-instantaneous rates. The system must be able to handle a variable volume and rate of data collection. Especially when under degradation or substantial attack, the data volume can grow exponentially. The system must be able to filter incoming data to collect only relevant data at a given moment, discarding useless information, and if needed, keeping the system performance within acceptable limits.

76. The system should identify and check incoming data. Data will need to have time/geospatial stamps and be signed to ensure authenticity and integrity, ensuring the trust of the source, and fulfill legal requirements. Standards should be developed for data feeds, especially for information sharing among the cyber centers. The system must be able to handle industry standard formats, and even unstructured data. Standards must be interoperable and flexible to ensure evolution when needed. The systems should be able to use data mining tools to gather information from available sources. Data extraction tools (i.e. semantic tools) should be used to extract data from those sources, but also to remove background noise.

77. There should be a capability to translate information from various languages into the language used by the cyber center.

Normalization

78. Data format standards must be developed to store data in a common format, to ensure comparability over time, across different sources and domains, and establish baselines. Data normalization should process both machine readable and human readable data (i.e. normalization to a common encoding of textual data to ensure correct analysis without loss of information). Normalization must be able to spot anomalies in incoming data and alert the cyber center for manual supervised processing and feedback to the original source.

Categorization

79. Technologies will need to check and apply meta-tagging and indexing on the data or information collected, following approved procedures and updating or refreshing the existing categorization tagging labels. The technologies will also need to be cognizant of collecting, handling and generating sensitive data, especially when data becomes classified in terms of commercial propriety, related to private individuals, or highlights critical national infrastructure. The declassification of sensitive information will impact on future retention and storage

requirements. The processes for undertaking these should largely be automated, but will require flexibility for manual setting of limits and conditions.

Aggregation

80. Technologies will need to check for duplication of data and manage configuration control to reduce storage needs and improve quality of analysis. Technologies will need to combine and fuse different meta-data to improve the quality of data.

81. Technologies will need to index data and meta-data to speed up retrieval. Support for unstructured data indexes and free searching must be provided. Technologies will need to sort data on categories and route them to proper storage.

Storage

82. Technologies will need to have large storage capacity. To buffer incoming data and avoid data loss, technology must provide temporary storage.

83. Technology should provide an efficient way to manage the required retention period and should be able to swap outhistorical data to a more cost-efficient storage tier. Technology must provide a retrieval rate and speed to fulfill both the data collection and analysis performance requirements.

84. Technology must provide security, access control and audits to ensure integrity and confidentiality of data. Technologies must ensure high availability, uninterrupted service to retrieve data, providing backup or replication services in case of either deliberate or accidental corruption or data loss.

## DETECTION AND ASSESSMENT

85. Information processing tools can be divided into three categories (1) data and event analysis, (2) operational visualization and (3) impact analysis and simulation. At the cyber center level, data flow analysis is a secondary task while the center concentrates on building SA using information collected from the ICT operators or other relevant information sources.

Data and Event Analysis

86. Data and event analysis technologies must require the capabilities of analyzing data in real time with 6 months of data available. Immediate access and historical data must be available for access within 2 - 3 hours. For each data element or event, a tool must calculate the high, low and average values over the following timeframes (e.g. 1 hour, 1 day, 1 week and 1 month). Technology must support network flow analysis and event analysis.

87. Technology must provide a real time data analysis against thresholds using various information techniques such as neural network and adaptive learning techniques to identify and flag abnormal events and attributes. Technology must also aggregate and calculate trend information.

Operational Visualization

88. Technology must visualize abnormal events, attributes, and trends. The events, attributes and trends could be displayed in text, tables, and graphs. The visualization functions include real-time data with overlay of corresponding baselines. Technology provides an ability to identify and display threats (vulnerabilities, malware, etc.), dependencies and interdependencies using correlated data from CERT and other threat related databases.

Impact Analysis and Simulation

89. Technology has the capability to conduct or support impact analysis and simulations to assess impacts and risks of network or infrastructure changes, and also conduct simulations to assess impacts of new threats or threat vectors.

## DISSEMINATION

90. Technologies should fulfill the following requirements for categorizing information:
- Capture, receive, or retrieve analysis output
- Tag or re-tag data
- Ability to filter and sort
- Ability to store data

91. Technology should provide an ability to remove sensitive data prior to dissemination, modify data, and translate documents into other languages. Technology should also provide an ability to manage profiles (language, sensitivity, frequency, inheritance), prioritize message traffic based on DMCIR and profiles based on user feedback.

## IMPLEMENTATION CHALLENGES

92. Underlying assumptions (paragraphs 6, 7 and 8) in most cases are not representative in a current organizational environment.

93. Resources to purchase and operate large scale technologies may be difficult in financially constrained environments.

94. Scientific solutions may be impossible for systems to achieve, especially at the high performance requirements.

95. Interoperable systems may be difficult to establish, but this may be overcome by open architecture systems. Standards need to be developed to collect and exchange data, and will need to be agreed upon.

96. Development and implementation of technologies may become obsolete before completion and not meet the requirements needed at the time.

97. Training and education burden of technologies employed will need to be overcome. A cadre of human specialists will be difficult to maintain with the appropriate skills and competencies.

98. Operating within national and international legal frameworks and legislation for collecting and storing data is a challenge.

99. A challenge is how actors understand cyberspace and its activities. It may be challenging to establish a dynamic and detailed portrayal of cyberspace activities on demand, with the ability to switch to an abstract view if required. Lack of cyber situational awareness tools and capabilities and thus lack of understanding cyberspace activities makes it hard for decision makers to understand which kind of value the cyber center provides. Lack of common understanding and existing models for mapping complex and adaptive systems to demonstrate dependencies, interdependencies and vulnerabilities may cause challenges.

## PART 6 – SUMMARY AND CONCLUSION

100. The purpose of the Cyber SA SOP is to describe how cyber situational awareness (SA) is established, maintained and shared in a generic, governmental cyber center. The cyber center collects information from various ICT operators, partner, and other cyber centers, analyses the information and shares the generated situational awareness to all relevant stakeholders. The Cyber SA SOP describes what information, reporting and collaboration is needed to build cyber situational awareness and to inform other relevant stakeholders - especially senior leaders, decision makers, and relevant ICT operators and partners.

101. The Cyber SA SOP describes a general SA process model with three process phases; collection, detection and assessment, and dissemination. The collection phase includes all activities that are related to information gathering. The cyber center uses all available and relevant information sources.

102. The Cyber SA SOP attempts to present a scalable SA process model that could be implemented in various environments e.g. military, commercial and government. A challenge is to define a model with sufficient details and at the same time, keep the model scalable and suitable for each individual environment.

103. Information sharing requires that all the stakeholders trust each other and have interoperable communications tools. Thus, technology solutions cannot solve information sharing problems if the stakeholders do not trust each other.

104. The Cyber SA SOP represents technology requirements and implementation challenges. There are already technologies that support required functionalities, but a problem is that implementation may be too complex and expensive. One of the challenges is lack of understanding which information is important and critical. The role of the cyber center is to serve higher level decision makers. Thus, it is vital that the decision maker is able to define critical information requirements.

ANNEX A

# DEFINITIONS

Cyberspace
Cyberspace is a global domain within the information environment. It consists of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. *(MNE 7 Campaign Plan; USA Deputy Secretary of Defense Memorandum, Subject: "The Definition of Cyberspace"; 12 May 2008)*

Cyber Situational Awareness
The perception of environmental elements with respect to time and/or space, the comprehension of their meaning, and the projection of their status after some variable has changed, such as time. Situational awareness involves being aware of what is happening in the vicinity to understand how data and information, network events, and SOCs' own actions will affect goals and objectives, both immediately and in the near future.

Cyber Center
A center where cyberspace activities are monitored and managed. The center provides a Cyber common operating picture (COP) and launches incident management activities. The center includes technical systems, personnel and procedures. The primary role of the center is to protect organizations, networks and services against intelligence collection and information exfiltration, and network attacks conducted by hostile or unauthorized users.

Cyber Center SA element
The cyber center SA element is a part of the cyber center, and is responsible for providing situational awareness of cyberspace activities. It has no executive decision making role within the cyber center.

Cyber Center SA Operator (SA Operator)
A person, who gains situational awareness of cyberspace activities and informs higher level decision-making.

System Operation Center (SOC)
A system operation center is any organization which has its own IT security organization/ structure that operates and/ or administrates parts of the global cyber infrastructure. The SOC may be governmental, non-governmental or private actor. [1]

Decision-maker
Senior leaders who are responsible for ongoing or future operations, whether military, government or commercial in cyberspace, and have to direct an appropriate response.

Event
A possible action that a system or user can perform that is monitored by a specific tool (application) or human operator.[2]

[1] **Operator (MNE 7 Cyber Legal Lexicon v0.1):** Means an undertaking providing or authorised to provide a public communications network or an associated facility. (Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive). Web 04.10.2011. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0007:0007:EN:PDF).

Incident

A cyber incident is an unwanted, unexpected or suspicious event that can have significant probability of compromising cyberspace activity or cyberspace information.[3]

Collaborative information sharing

Collaborative information sharing covers the real-time communication between SOCs while conducting cyber activities, and the methods on how information can be leveraged by higher level cyber center SA operators. In addition to collaborative information sharing, information is also collected through traditional reporting mechanisms.

[2] **Event (Wikipedia):** An observable occurrence, phenomenon or an extraordinary occurrence

[3] **Cyber Incident (MNE 7 Campaign Lexicon v0.2):** An incident that causes, or is likely to cause, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or threatens public health or safety, undermines public confidence, has a negative effect on the national economy, or diminishes the security posture of a nation. *(UK Government working definition)*